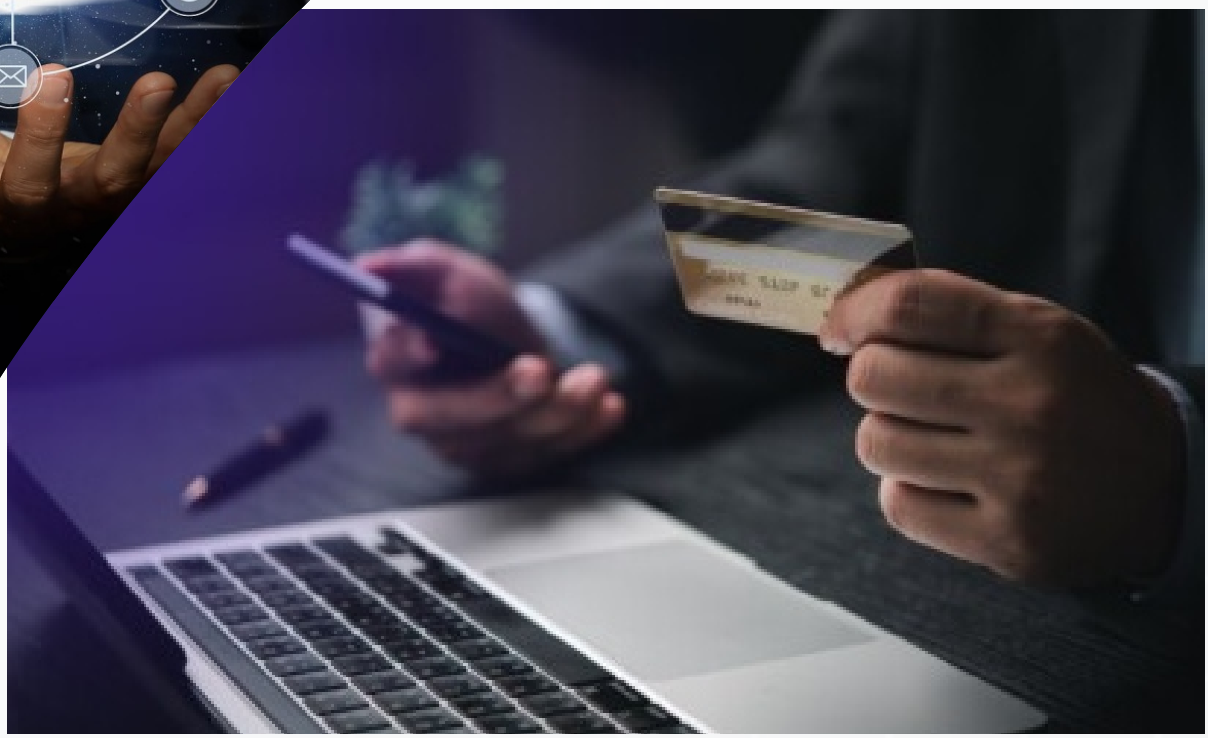
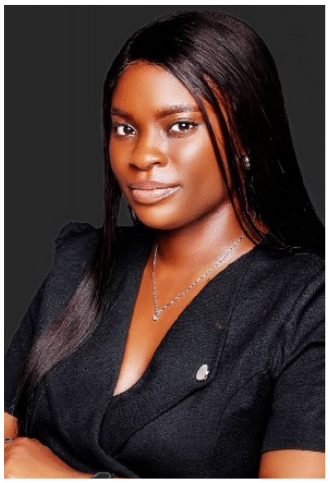
PINHEIRO LP



REGULATORY FRAMEWORKS:

CURBING FRAUD IN THE FINTECH INDUSTRY THROUGH COMPLIANCE

Authors



Ronke Fapohunda
Associate Partner
Pinheiro LP

Boluwatife Popoola
Senior Associate
Pinheiro LP

1.0 INTRODUCTION

The Nigerian Fintech space has experienced significant growth driving financial inclusion and innovation and it is refreshing to see that we are finally "banking the unbanked" and incorporating more people into the financial system in Nigeria. In the last five years, the industry has produced four (4) Unicorns - Flutterwave, Paystack, Kuda Bank, Opay.

The fintech revolution has changed how money moves—fast, borderless, and digital. But with innovation comes risk. In just seconds, a cybercriminal halfway across the world can drain accounts, manipulate transactions, or exploit loopholes in digital finance systems. The result? Billions lost, reputations shattered, and consumer trust eroded. The surge in fraud within Nigeria's Fintech Industry has necessitated regulatory interventions from key financial regulators such as the Central Bank of Nigeria (CBN), and the Securities and Exchange Commission (SEC) who are issuing compliance guidelines to curb illicit practices. Effective regulatory compliance is critical in maintaining public trust and ensuring financial system stability and prevent a recurrence of banking crises.

This was affirmed by the Supreme Court in **A.G Lagos State v Eko Hotels Ltd.** where the court emphasized that regulatory compliance is fundamental for industries affecting economic stability.

This article dives into how smart regulations, backed by cutting-edge compliance strategies, can protect businesses, customers, and the integrity of the global financial. It also highlights the positive impact of adopting key international legal standards within Nigeria's regulatory regime.

2.0 SITUATION REPORT ON FINTECH FRAUD IN NIGERIA

Recent reports indicate a dramatic surge in fraudulent attacks on and within the Nigeria Fintech Sector, as criminals increasingly exploit the flexibility of these platforms. For example, losses attributable to fraud rose from 468.49 million in Q1 2024, to 42.6 billion in Q2 2024. For context, this is about nine hundred percent (900%) increase in less than a year. These figures justify the intensified efforts by financial regulators to restore sanity in this crucial sector of the economy.

Fraudulent activities in the Fintech industry takes various forms.

The strategies deployed range from **identity theft** where criminals steal customers information to open accounts or perform unauthorized transactions, to **Insiders' fraud**—where employees abuse access to initiate fraudulent transactions against the customers or the company and, **Money laundering** which is the transfer of money incurred via illicit activities through several channels to obscure the illegitimate source with the sole aim of integrating it into the financial system violating the **Money Laundering (Prevention and Prohibition) Act, 2022**. Other reported cases involve - payment fraud, loan and credit facilities, phishing scams, investment scams, chargeback fraud etc. These trends necessitate a robust, multi-faceted regulatory response to safeguard investors, consumers, and the entire financial system.

1. (2017) LPELR-43713(SC)
2. FITC "Reports on Fraud and Forgeries in Nigerian Banks" (2024). Available at < https://fitc-ng.com/wp-sscontent/uploads/2024/09/Fraud-and-Forgery-2024-2nd-Quarter.pdf> Accessed (January 22, 2025).

3.0 REGULATORY FRAMEWORK IN THE FINTECH INDUSTRY

Nigeria's banking and fintech sectors are among the most regulated sectors in the country. Fintech companies, as corporate entities, are subject to scrutiny under various Acts, including the **Companies and Allied Matters Act 2020**, which establishes corporate governance requirements.

Additionally, sectoral regulations such as the **Banks and Other Financial Institutions (BOFI) Act of 2020**, the **Central Bank (CBN) Act** 2007 exist, and they provide oversight for financial institutions and mandate strict compliance with CBN guidelines.

This was seen in **Fidelity Bank v Bayuja Ventures Ltd,** where the Court held that a bank cannot unilaterally freeze a customer's account without obtaining a court order - even if fraud is suspected. The bank's failure to adhere to the CBN's Regulatory Framework for Bank Verification Number (BVN) and Watchlist for the Nigerian Banking Industry (2017) and the CBN Customer Due Diligence Regulations (2023) resulted in illegality and liability for wrongful account restrictions.

The Investment and Securities Act (ISA) 2007, also governs capital markets operations, including those affecting FinTech's firms.

Moreover, specific regulations ensure the sanctity of the financial sector, such as the **Nigerian Data Protection Act 2023 (NDPA)**, ensure the security and privacy of customer data, as emphasized in **Section 24 and Section 38**, which mandates strict data protection methods. Additionally, the **Anti-Money Laundering (AML) Act 2023,** and **the CBN Know-Your-Customer (KYC) Regulations,** which mandate rigorous guidelines in ensuring identity verification and transaction monitoring to curb and money laundering.

4.0 INTER-AGENCY REGULATORY COLLABORATION

Effective regulatory oversight requires a structured framework for collaboration among key regulatory bodies, including the CBN, SEC, NFIU and the National Data Protection Commission (NDPC). Enhanced coordination, information sharing, and joint enforcement and efforts among these agencies are imperative to ensure a comprehensive and proactive response to evolving complexities of financial fraud. The Supreme Court **in A.G**

3.Chimgozirim Nwokoma "Exploring the surge in fraud in Nigeria's burgeoning fintech industry" (2024). Available at < Https://Techpoint.Africa/2024/09/18/Fintech-Fraud-Nigeria/> Accessed (January 23, 2025).
4.(2019) LPELR-46420 (CA)

Federation v A.G Lagos State highlighted the necessity of inter-agency collaboration in sectors with overlapping regulatory oversight when it emphasized the importance of collaboration between federal and state regulatory agencies to ensure effective governance.

This decision reinforces the importance of the synergy among the regulatory agencies in tackling financial fraud and other issues requiring multi-agency oversight.

5.0 COMPLIANCE RECOMMENDATIONS: CURBING FRAUD IN FINTECH

To mitigate fraud in Fintech, it has become imperative not just for Fintech's but for companies to adopt a multi-layered compliance framework covering the following areas:

5.1 Adoption of Contractual Clauses Mandating Regulatory Technology (RegTech) Integration for Third-Party Service Providers

In line with data protection and outsourcing guidelines under the NDPR and CBN Guidelines for the Regulation of Agent Banking and Operations in Nigeria, fintech's should include strict contractual provisions requiring third-party vendors (e.g., KYC software, payment gateways) to use RegTech tools for real-time fraud detection and regulatory reporting. This ensures that liability is properly allocated and that Fintech's remain compliant with outsourcing obligations. These clauses should include indemnities, audit rights, and breach reporting protocols to manage third-party risk legally and effectively.

5.2 Data and Information Security

Fintech companies must build "digital values" that mirror the physical security of traditional banking. Given the vulnerability of digital platforms, companies are responsible for implementing robust data and information compliance protocols.

On the issue of data protection, unauthorized access to personal data can lead to fraud and highlighted system vulnerabilities. In accordance with **Section 24 of the NDPA**, all data controllers are mandated to process data in a "manner that ensures appropriate security".

Section 38 further mandates that financial institutions must maintain systems ensuring data security, integrity and confidentiality.

Annual audits of data protection compliance, as required by the NDPR 2019 are also essential.

Additionally, the CBN's 2021 blueprint prescribes the standards expected of payment service providers and even microfinance banks. Adherence to **ISO 27001/27002, (information security) — ISO 27032, (cyber security) — ISO 27017 (cloud security)**. is crucial.

5.(2013) LPELR- 20974 (SC)
6.Nigerian Data Protection Act, 2023.
7.Regulation 4.1(7) of the Nigeria Data Protection Regulation 2019.

8.CBN "Nigerian Financial Services Industry IT Standards Blueprint for Payment Service Providers (PSPs) and National Microfinance Banks (NMFBs)" Available at; <https://www.cbn.gov.ng/itstandards/IT_Standards_Blueprint%20for%20Payment%20Solution%20Providers%20(PSPs)%20and%20the%20National%20Microfinance%20Banks%20(NMFBs)%20%20version%201.1.pdf> (Accessed January 18, 2025).
9.Unity (2016) LPELR- 40064 (CA)
10.(2012) LPELR – 21138 (CA)Z

As seen in the case of **Oceangate Offshore Services Ltd V MT,** where failure to protect customer data led to a liability, the Court held in favour of Oceangate Offshore Services, awarding damages to compensate for the losses incurred as a result of data breach.

5.3 Anti-Money Laundering (AML) / Know Your Customer (KYC) Policy

Fintech companies must maintain robust AML/KYC policies to mitigate fraud and prevent terrorism funding. Asides the fact that this practice is in line with global best practices, it is also in line with some existing laws and guidelines in Nigeria regulating internal activities of financial institutions. For example, it is in line with the **Money Laundering (Prevention and Prohibition) Act of (MLA) 2022**. The idea of these regulations and legislations is to prevent and minimize anonymous transactions such that there is transparency, and every transaction can be linked to the persons, and institutions initiating them.

In practice, these are not some self-implementing regulations, and neither are they mere abstract concepts. In terms of implementation, Fintech companies are expected to demand verification from customers, as this amounts to them exercising appropriate due diligence, as seen in the case of **First Bank of Nigeria v Owie**, where the court emphasised the responsibility of financial institutions to exercise due diligence in transactions. These verifications are usually made to enable the companies to determine who the customers really are. For example, verifying government-issued information such as the National Identification Number (NIN), Bank Verification Number (BVN). While this is the first step, it goes beyond that to include monitoring and reporting suspicious financial activities to the Nigerian Financial Intelligence Unit (NFIU). Fintech companies should hire highly trained professionals to offer these compliance services and engage services of consultants specializing in these areas such as auditors and compliance consultants.

5.4 Technical Fraud Detection Infrastructure

Cyberattacks and fraud in the Fintech industry are increasing both in frequency and sophistication. Companies must deploy robust technical measures to safeguard customer data and transactions. With emerging technologies like Artificial Intelligence, it is expected that these illegalities would increase, but Fintech can mitigate this risk by equally deploying AI tools for efficient fraud detection and data and information security to protect its systems from attacks and breaches e.g. two-factor authentication.

This infrastructure should also include public notices which promotes safe and security-conscious behaviours with the customers. For example, regularly updating Mobile Applications when security incidents have been recognized and fixed is recommended.

Also, ensuing that only strong passwords which are difficult to be "brute-forced", as well as mandatory 2-factor authentication. These and other ingenious strategies should be deployed by Fintech companies to detect fraud and protect customers from losing their resources. It should be noted that failure to implement robust security measures may expose the firms to legal claims, as seen in **Diamond Bank Ltd v Partnership Investment Co. Ltd**, where the court found a direct causal link between the Bank's inadequate security measures and the financial losses incurred by Partnership Investment Co. Ltd, leading to a ruling that held the bank liable for compensatory damages.

5.4 EMERGING TECHNOLOGIES FOR FRAUD PREVENTION

Leveraging cutting-edge technology is critical in the fight against fraud. Fintech companies should deploy AI-driven systems that analyse large datasets in real time to identify anomalous patterns indicative of fraudulent activities. In addition, integrating blockchain technology can enhance transaction transparency and traceability through its decentralized, tamper-resistant ledger capabilities. Continuous investment in these emerging technologies is essential to remain ahead of evolving fraud tactics. The necessity of adopting advances fraud prevention technologies was highlighted in **UBA V Jargaba,** where the Supreme Court stressed the duty of financial institutions to safeguard customer funds through technological advancements.

5.5 CONSUMER PROTECTION AND EDUCATION

Empowering consumers is a vital defence against fraud. This can be achieved by developing initiatives that educate consumers on identifying and preventing fraudulent activities, using diverse channels such as social media and community outreach. Fintech companies should also integrate educational content and best practice guidelines into their mobile apps and websites to further enhance consumer awareness and protection.

Furthermore, providing accessible information on consumer rights and establishing dedicated support channels for fraud victims are crucial measures, thereby providing a clear dispute resolution mechanism, as mandated by the CBN Consumer Protection Framework.

6.0 COMPARATIVE GLOBAL REGULATORY FRAMEWORKS FOR COMBATING FINTECH FRAUD IN NIGERIA

To effectively curb the persistent threat of fraud in Nigeria's burgeoning Fintech sector, it is imperative to examine and draw insights from global best practices and established regulatory models. Countries such as the United Kingdom, the United States, Ghana, and South Africa have pioneered

11.(2009) 18 NWLR (pt.1172)67
12.(2007) LPELR- 3399 (SC)

innovative compliance structures tailored to their Fintech ecosystems. Additionally, international protocols offer a harmonized baseline to guide cross-border financial integrity and enforcement. By aligning with these standards and adapting them to local realities, Nigeria can foster a resilient and fraud-resistant fintech landscape.

6.1 United Kingdom: Risk-Based Supervision and FCA Oversight.

The United Kingdom's Financial Conduct Authority (FCA) established by the **Financial and Markets Act 2000**, exemplifies a balanced approach to fintech oversight, employing a risk-based supervision framework that prioritizes both innovation and systemic risk mitigation. Through its Handbook—particularly the **SYSC (Senior Management Arrangements, Systems and Controls) Rules**—the FCA mandates that regulated entities establish effective internal systems and controls to combat financial crime. The Money Laundering Regulations 2017 (as amended) further require robust Know-Your-Customer (KYC) protocols and transaction monitoring mechanisms.

It is important to note that the SYSC in conjunction with other regulatory measures like the Payments System Regulator (PSR) and Strong Customer Authentication (SCA) have been successful in increasing the investments in fraud prevention measures and the decline in overall fraud losses. Hence, Nigeria should consider such an interplay between multiple preventive measures, ensuring they are employed together.

6.2 United States: Multi-Layered Oversight and FinCEN's AML Obligations.

In the United States, fintech regulation operates through a decentralized yet stringent framework, anchored by the Bank Secrecy Act (BSA) and enforced by the Financial Crimes Enforcement Network (FinCEN). The BSA imposes specific AML obligations on fintech's, including:

i. 31 U.S.C. 5318: Requires financial institutions, including fintech entities, to implement AML programs that are designed to detect and report suspicious activities, and prevent money laundering and financing of terrorism.

ii. 31 U.S.C. 5318(g): This mandates financial institutions to file Suspicious Activity Reports (SARs) when they detect transactions that they believe may involve money laundering or other illicit activities. This is a critical compliance requirement for fintech firms under BSA.

The IRS Criminal Investigation division of FinCEN also reported a recovery of $21.1 billion of fraudulent assets between 2022 and 2024 showcasing the BSA's role in facilitating such recoveries.

The key lesson here for Nigeria is that agencies such as the NFIU and the NDPC should enhance intelligence-driven enforcement and support the development of AI-powered SAR systems and dynamic transaction flagging tools in order to have such results.

6.3 Ghana: Tiered Licensing and Digital Onboarding Compliance.

Ghana's **Payment Systems and Services Act, 2019** presents a progressive framework that introduces tiered licensing for Fintech operators, balancing financial inclusion with systemic risk control. The Bank of Ghana enforces real-time monitoring of suspicious transactions and requires integration with national identity databases for effective digital onboarding.

This dual strategy of enabling broad access while maintaining stringent fraud controls offers a pragmatic model for emerging economies. Therefore, Nigeria's CBN should explore a modular licensing regime for Fintech's, coupled with enhanced digital identity verification systems and API-level audit trails to ensure transparency and traceability in Fintech operations.

6.4 South Africa: Inter-Agency coordination via IFWG.

South Africa has institutionalized inter-agency cooperation through its Intergovernmental Fintech Working Group (IFWG), which facilitates regulatory cohesion across key institutions. This comprises representatives from South African Reserve Bank, Financial Sector Conduct Authority, Financial International Centre, National treasury, National Credit Regulator etc.

Using, Financial International Centre, as a case study, **Financial Intelligence Centre Act (FICA) 2021** imposes robust AML and counter-terrorism financing (CTF) obligations on accountable institutions, including Fintech firms. For Nigeria, there is a critical need for the establishment of a multi-agency fintech taskforce, modelled after South Africa's IFWG to harmonize compliance standards and enable coordinated responses to systemic fraud and financial crime in the fintech sector.

6.5 International Protocols: FATF, GDPR, IOSCO.

Globally, Nigeria must align with a set of overarching international standards. Among the most significant of these are the **Financial Action Task Force (FATF), the European Union's General Data Protection Regulation (GDPR), and the International Organization of Securities Commissions (IOSCO)**. These standards influence global financial practices, and their relevance to Nigeria, particularly in its evolving Fintech sector, is increasingly paramount.

i FATF – 40 Recommendations:

Compliance with the Financial Action Task Force's 40 Recommendations, especially on digital KYC and beneficial ownership transparency, is essential for Nigeria's global financial credibility. These recommendations provide a roadmap for Nigeria to align with international standards and bolster its regulatory framework in the fintech sector.

ii. GDPR: The EU's General Data Protection Regulation serves as a model for privacy-by-design and breach notification principles, both of which have influenced Nigeria's own **NDPA 2023**. While not directly binding on Nigeria, the GDPR's influence is significant, especially for Nigerian Fintechs dealing with EU customers.

iii. IOSCO: Serves as the primary global standard-setter for securities regulation, with a core mandate to promote investor protection, ensure market integrity, and mitigate systemic risk across jurisdictions. These objectives are particularly pertinent to Nigeria, given its expanding digital asset ecosystem and increasing participation in cross-border capital markets. The IOSCO Objectives and Principles of Securities Regulation (2017) outline three key goals: (i) investor protection, (ii) fair, efficient, and transparent markets, and (iii) the reduction of systemic risk. These goals are reflected in the SEC Nigeria Regulatory Framework for Digital Assets (2022), which seeks to regulate digital asset offerings and ensure market integrity.

iv. To fully align with IOSCO standards, Nigeria would benefit from institutional reforms and the establishment of robust bilateral and multilateral cooperation frameworks. Strengthening cross-border enforcement capabilities is essential for enhancing investor confidence, improving regulatory credibility, and supporting Nigeria's integration into the global financial system in line with international best practices.

7.0 CONCLUSION

Nigeria's Fintech Industry must balance innovation with compliance to prevent financial fraud. Regulatory compliance is not optional- it is mandatory to protect consumers, ensure market stability, and prevent systemic risks. As seen in **CBN V Okojie**, non-compliance with financial regulations can lead to sanctions, liability and reputational damage.

By aligning with domestic requirements and global best practices, Fintech firms can create a resilient and fraud- resistant ecosystem in Nigeria that fosters sustainable growth and innovations.

Furthermore, Nigeria's regulatory framework is increasingly aligning with international standards set by FATF, GDPR, and IOSCO. The Nigerian MLA 2022, CBN AML/CFT Guidelines, and NDPA reflect a commitment to combating financial crimes and safeguarding data privacy. However, gaps persist, particularly in cross-border enforcement cooperation and formalizing international regulations.

Strengthening these areas will be crucial as Nigeria develops its fintech sector and engages in global financial markets.

By further aligning with global standards, Nigeria can enhance its regulatory framework, build investor confidence, and provide robust protection against emerging financial risks.

2015) LPELR – 24740 (CA)

www.pinheirolp.com